Exam : MS-102

Title : Microsoft 365 Administrator

https://www.passcert.com/MS-102.html

1. Topic 1, Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 ES subscription.

Existing Environment

Requirement

The network contains an on-premises Active Directory forest named contoso.com.

The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops are Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Name	Azure AD role
User1	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Planned Changes

Contoso plans to implement the following changes:

• Implement Microsoft 365.

• Manage devices by using Microsoft Intune.
• Implement Azure Advanced Threat Protection (ATP).
• Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

Technical Requirements

Contoso identifies the following technical requirements:
• When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automaticity.
• Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
• User1 must be able to enroll all the New York office mobile devices in Intune.
• Azure ATP sensors must be installed and must NOT use port mirroring.
• Whenever possible, the principle of least privilege must be used.
• A Microsoft Store for Business must be created.

Compliance Requirements

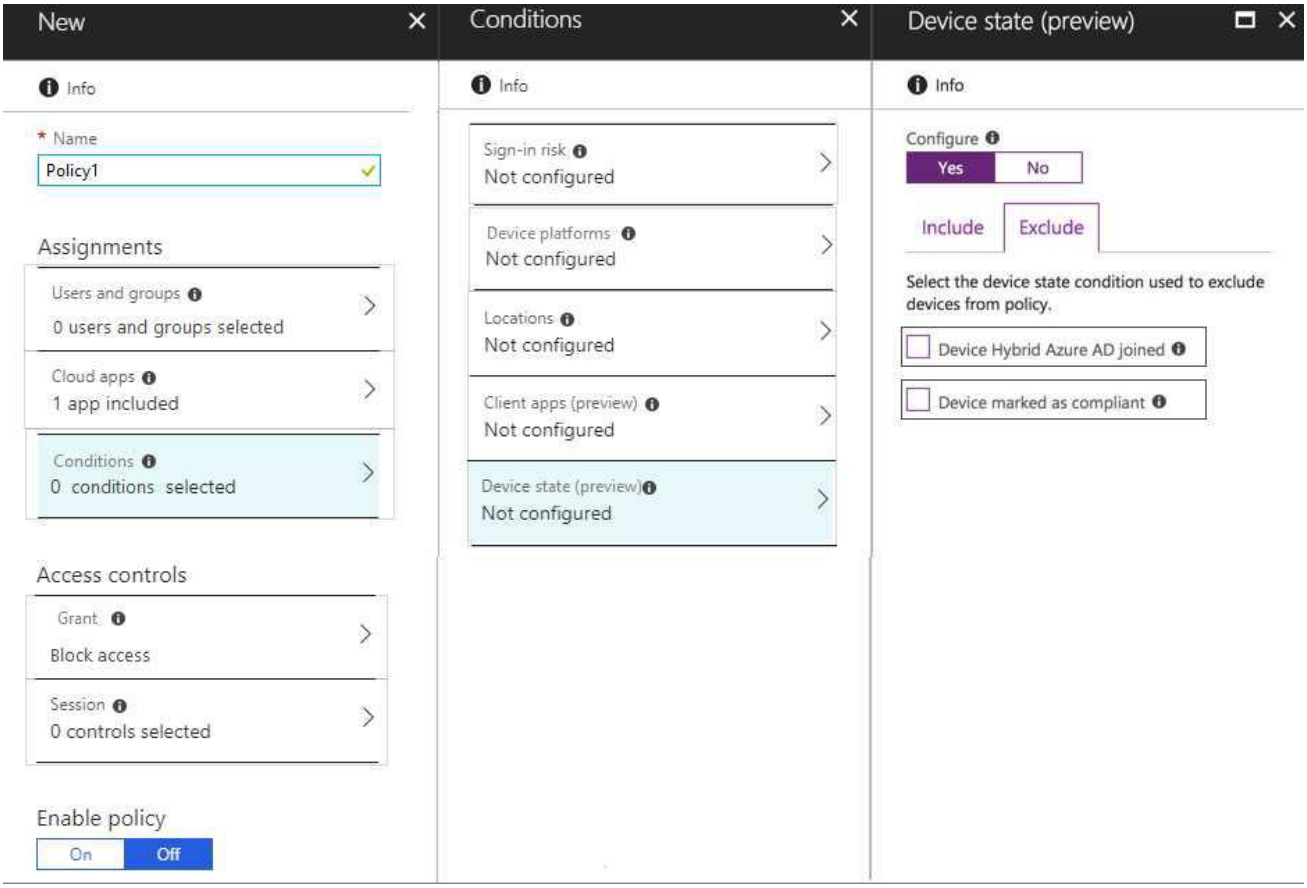
Contoso identifies the following compliance requirements:
• Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
• Configure Windows Information Protection (W1P) for the Windows 10 devices.

HOTSPOT

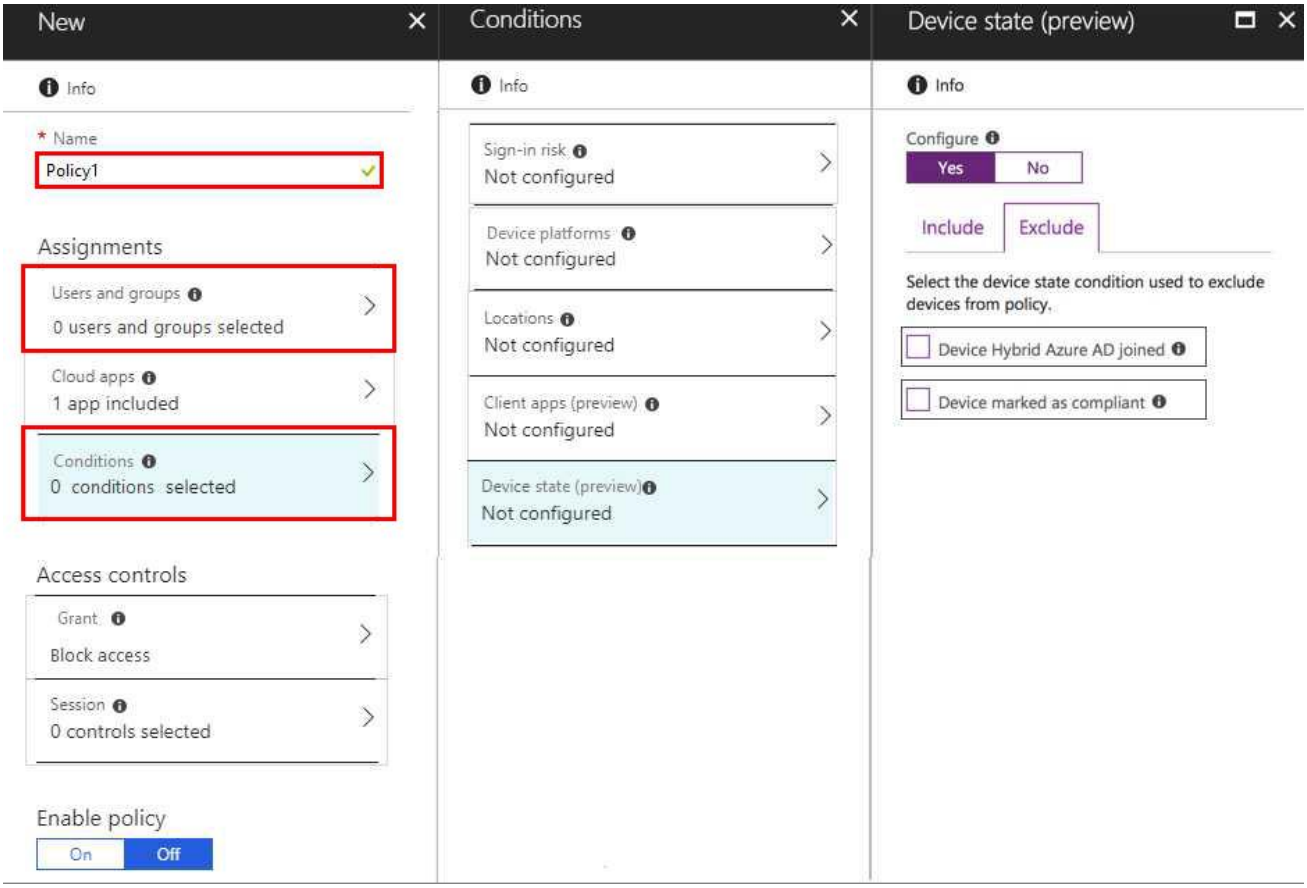
You need to configure a conditional access policy to meet the compliance requirements.

You add Exchange Online as a cloud app.

Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.


New
Info
* Name
Policy1
Assignments
Users and groups
0 users and groups selected
Cloud apps
1 app included
Conditions
0 conditions selected
Access controls
Grant
Block access
Session
0 controls selected
Enable policy
On
Off
Conditions
Info
Sign-in risk
Not configured
Device platforms
Not configured
Locations
Not configured
Client apps (preview)
Not configured
Device state (preview)
Not configured
Device state (preview)
Info
Configure
Yes
No
Include
Exclude
Select the device state condition used to exclude devices from policy.
Device Hybrid Azure AD joined
Device marked as compliant

Answer:


New
Info
* Name
Policy1
Assignments
Users and groups
0 users and groups selected
Cloud apps
1 app included
Conditions
0 conditions selected
Access controls
Grant
Block access
Session
0 controls selected
Enable policy
On
Off
Conditions
Info
Sign-in risk
Not configured
Device platforms
Not configured
Locations
Not configured
Client apps (preview)
Not configured
Device state (preview)
Not configured
Device state (preview)
Info
Configure
Yes
No
Include
Exclude
Select the device state condition used to exclude devices from policy.
Device Hybrid Azure AD joined
Device marked as compliant

Explanation:
Reference: https://docs.microsoft.com/en-us/intune/create-conditional-access-intune

2.On which server should you install the Azure ATP sensor?
A. Server 1
B. Server 2
C. Server 3
D. Server 4
E. Server 5
Answer: A
Explanation:
Reference: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning
However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

3.You need to meet the compliance requirements for the Windows 10 devices.
What should you create from the Intune admin center?
A. a device compliance policy
B. a device configuration profile
C. an application policy
D. an app configuration policy
Answer: C

4.HOTSPOT
You need to meet the Intune requirements for the Windows 10 devices.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Settings to configure in Azure AD:

Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

Answer:

Settings to configure in Azure AD:

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority

Explanation:

Reference: https://docs.microsoft.com/en-us/intune/windows-enroll

5.HOTSPOT

As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Seattle:

- 6 months
- 18 months
- 24 months
- 30 months
- 5 years

New York:

- 6 months
- 18 months
- 24 months
- 30 months
- 5 years

Answer:

Explanation:
https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet March Feature Updates: Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date
Reference:
https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

6.You need to ensure that User1 can enroll the devices to meet the technical requirements.
What should you do?
A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator rote.
B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
C. From the Intune admin center, add User1 as a device enrollment manager.
D. From the Intune admin center, configure the Enrollment restrictions.
Answer: C
Explanation:
Reference:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

7.You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.
What is the minimum of dedicated support technicians required?
A. 1
B. 4

C. 7
D. 31
Answer: B
Explanation:
Reference:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

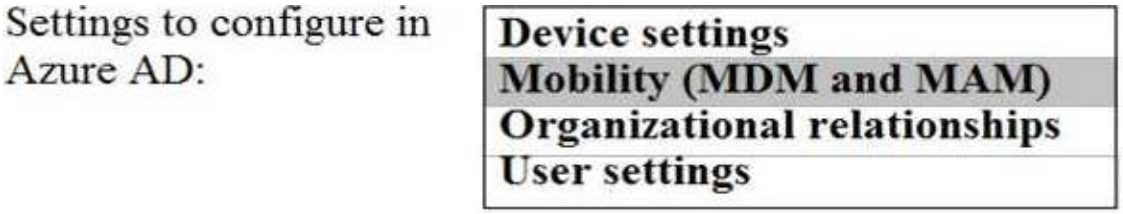
8.You need to create the Microsoft Store for Business.
Which user can create the store?
A. User2
B. User3
C. User4
D. User5
Answer: C
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

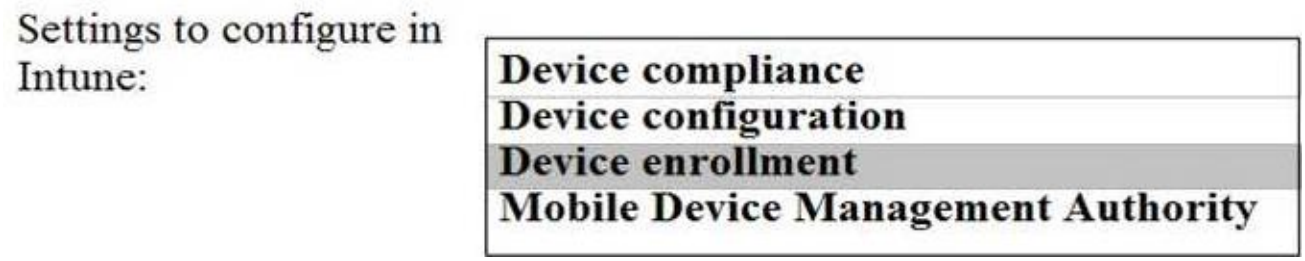
9.HOTSPOT
You need to meet the technical requirements and planned changes for Intune.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Settings to configure in Azure AD:	
	Device settings
	Mobility (MDM and MAM)
	Organizational relationships
	User settings

Settings to configure in Intune:	
	Device compliance
	Device configuration
	Device enrollment
	Mobile Device Management Authority

Answer:





Explanation:
Reference: https://docs.microsoft.com/en-us/intune/windows-enroll

10.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.
Does this meet the goal?
A. Yes
B. NO
Answer: A
Explanation:
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager. To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune.
Reference: https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable

11.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You create a device configuration profile from the Device Management admin center.
Does this meet the goal?
A. Yes
B. No
Answer: B
Explanation:
It looks like the given answer is correct. There is an on-premises Active Directory synced to Azure Active Directory (Azure AD) So the co-management path1 - Auto-enroll existing clients
1. Hybrid Azure AD
2. Client agent setting for hybrid Azure AD-join
3. Configure auto-enrollment of devices to Intune
4. Enable co-management in Configuration Manager
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-client

12.On which server should you use the Defender for identity sensor?
A. Server1
B. Server2
C. Server3
D. Server4
E. Servers5
Answer: A
Explanation:
However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

13. Topic 2, A. Datum

Case Study: Overview
Existing Environment
This is a case study Case studies are not timed separately. You can use as much exam time as you would

like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Current Infrastructure
A. Datum recently purchased a Microsoft 365 subscription.
All user files are migrated to Microsoft 365.
All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2#uk.ad3tum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.
A. Datum uses and processes Personally Identifiable Information (PII).

Problem Statements
Requirements
A. Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Business Goals
A. Datum warns to be fully compliant with all the relevant data privacy laws in the regions where it operates.
A. Datum wants to minimize the cost of hardware and software whenever possible.
Technical Requirements
A. Datum identifies the following technical requirements:
Centrally perform log analysis for all offices.
Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.

A security administrator requires a report that shows which Microsoft 36S users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive US. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

You need to meet the technical requirement for the EU PII data.
What should you create?
A. a retention policy from the Security & Compliance admin center.
B. a retention policy from the Exchange admin center
C. a data loss prevention (DLP) policy from the Exchange admin center
D. a data loss prevention (DLP) policy from the Security & Compliance admin center
Answer: A
Explanation:
Reference: https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies
EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

14.You need to meet the technical requirement for large-volume document retrieval.
What should you create?
A. a data loss prevention (DLP) policy from the Security & Compliance admin center
B. an alert policy from the Security & Compliance admin center
C. a file policy from Microsoft Cloud App Security
D. an activity policy from Microsoft Cloud App Security
Answer: D
Explanation:
Reference: https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts